International Journal of Emerging Research in Management &Technology
ISSN: 2278-9359 (Volume-3, Issue-6)

Research Article | **June 2014**

Continuous Touchscreen Mobile Authentication Using Several Gestures

Mr.S.M.Sangave*
Department of Computer Engineering
Dnyanganga College of Engineering & Research,
Narhe, Pune, India

Mr.B.A.Chaugule
Department of Computer Engineering
Dnyanganga College of Engineering &Research
Narhe, Pune, India

Abstract -

Recently mobile use is general to everyone, now a day's mobile is one of the basic needs of human being. Currently Touchscreen handheld devices are more popular because they have large storage capacity, fast internet access, high portability and user friendly. Number of peoples uses touchscreen mobile phones, tablets, PDA's for the different purposes such as accessing online data, net banking, storing personal data [bank account details, contact numbers , official data etc] . If such mobile is lost or stolen then it can be misuse by other peoples and also there is problem for recovering such the data. Hence providing security for such Smartphone devices, we are survey the techniques which provide security to the Smartphone devices. In this paper we are going to do survey the continuous mobile authentication process and techniques which are used for mobile authentication. We survey FAST (Finger gestures Authentication System using Touchscreen) technique for touchscreen mobile device authentication.

Keywords- Hand-held device, touch-screen Device, user authentication, FAST.

I. INTRODUCTION

1.1 Definition of mobile handheld devices:

Any handheld device that operates to hold, store, process, and access data, including smartphones, cellphones, tablets, or personal digital assistants (PDAs) used to conduct university business [4].

Today's phones already enable contactless payments, mobile wallets and mobile banking, and these changes are the indication the need for secure services that can be performed wirelessly or with a Smartphone [3]. Smartphone, tablets and other mobile devices continue to propagate and provide users with powerful, mobile network, multimedia computing options, hence the need to secure them. According to the handheld devices definition they are use for the storing data, accessing data that will be personal or social data. Recently the use of hand held devices increases because it provide large storage capacity also fast internet access speed. The study of over 6,000,000 passwords, 91% of all user passwords belong to a list of just 1,000 common passwords (e.g., 8.5% users use either "password" or "123456" as their passwords) [2]. Moreover, the additional hardware cost makes standard biometric authentication techniques to be still unpopular on mobile devices .Any handheld device that is used in combination with Cornell activities, including retrieval of email or calendar data must be configured so that it can be locked or erased if it is lost or stolen. To concentrate on the pressing demand for a more secure and user friendly mobile authentication solution technological advances in computing and I/O capabilities as well as network connectivity are shifting the focus from PCs to mobile devices.

Market analysis predicts that in 2015 there will be 1.5 billion smartphones and 640 million tablets in use worldwide [1], currently number of companies, universities, and colleges' uses portable Touchscreen mobile devices such as Smartphone's, Tablets, and laptops. Handheld devices are suitable to carry anywhere in the world and also it can be access everywhere so the popularity of hand held devices increases also the security issues are consider for increasing the popularity as mobile devices is easily lost or stolen, security of such devices is most important because we use such devices to store personal data, official data which is confidential to user. If it stolen then confidentiality of that user is lost and unauthorized user can misuse that information. Thus, the continuous or implicit authentication approach, which intelligently monitors and analyzes the user-device interaction to ensure the correct user, it can either complement the point based authentication or even substitute it if the approach satisfies particular accuracy requirements [2]. Touch traces are affected by two biometric features, i.e., the user hand geometry and the muscle behavior. The variations of biometric characteristics have the potential to provide user differentiation [8].

II. BACKGROUND

2.1 *Touch Based Continuous Mobile Authentication*

Today's in market there is number of Smartphone uses the pattern gesture security. They provide only single gesture pattern to the authentication, such single pattern authentication provide at the entry level only and the security of such Smartphone is not strong so for providing strong security, we need a continuous mobile authentication . Our basic aim to provide the strong security in Touch screen mobile devices.

Gesture reorganization uses the pattern matching process for the authentication in the number of Smartphone's that capture the specific pattern and compare with new one. If new pattern match with the captured ones then it give the authentication to the user but this will not be provide strong authentication to the user because suppose that device or

mobile is lost or stolen then any one can guess such pattern and crack that pattern gesture easily and it can misuse that handheld device. This can be happen because of there is only single gesture pattern and only entry level authentication process is available

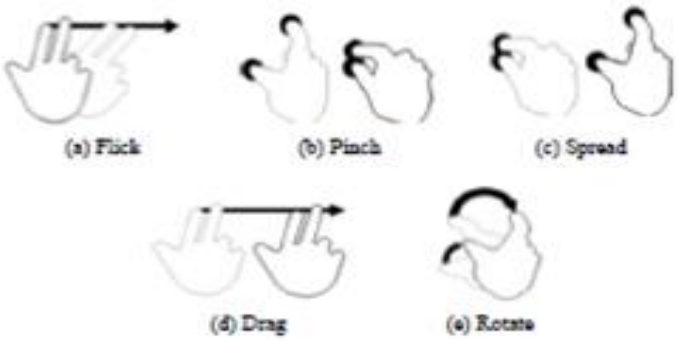


Fig. 1. Example Multi-touch Gestures

In pattern or gesture reorganization Patterns or gestures are the user specific and used for detecting the mobile users. Here the touch input gestures classified into three categories: touch gestures (e.g., flick, spread, pinch, drag, and tap) virtual typing (e.g., typing using a touch screen based keyboard, entering a phone number using touch); and touch Based drawing (e.g., drawing shapes using fingers). For each category, user specific features can be extracted from traces collected from a device touch screen, in this paper we mostly concentrate on only the touch gestures and the different type of touch gestures are shown in the fig.-1.In general when we start to use the biometric features for security at that time the basic processes is used in which we store the biometric feature firstly and compare when we want to authenticate the user.

Figure-2 shows the basic working of mobile authentication process, touchsceen is used for taking the input from the user that should be works by using touchsceen driver and API. The event capture module capture the gesture from the user and extract it with the enrolled gesture .Touch gesture engine provide the validation of new gesture for the authentication. If it matches then it provide authentication to the user if it does not match then abort the authentication.

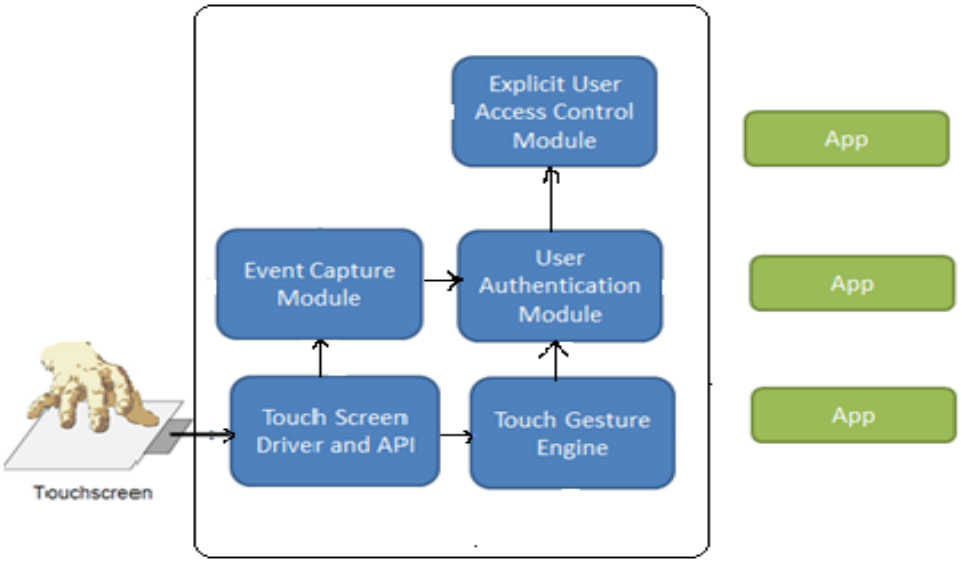


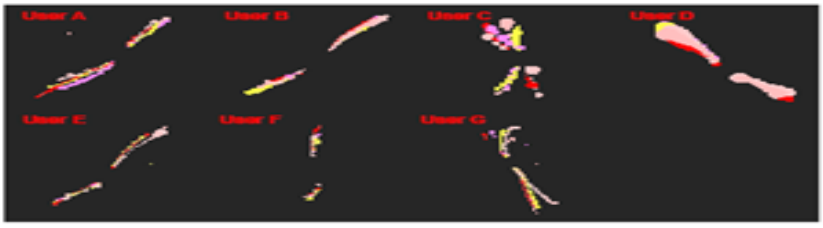
Fig. 1 The overview of the continuous mobile authentication system

III. THE FAST FRAMEWORK AND DESIGN

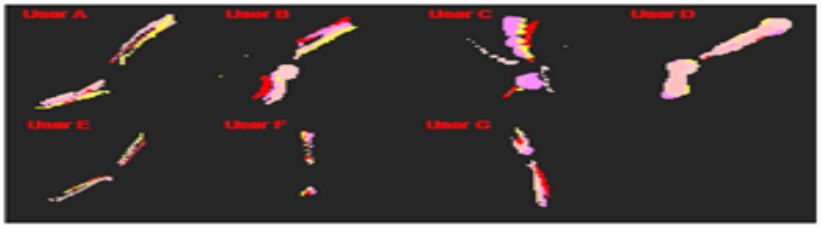
We know current Smartphone authentication process is at entry level only and it take only single gesture to authenticate the user. FAST (Finger gesture Authentication system using Touchscreen) is a touch gesture based user authentication system. It focuses on the post-login user authentication figure-2 shows the how the authentication process works and figure-1 shows some gesture samples. FAST authenticate the user continuously. FAST framework consists of the touchscreen for entering the gestures, sensor glove for reading the dots at the time of gesture drawing.

3.1 Touch Gestures

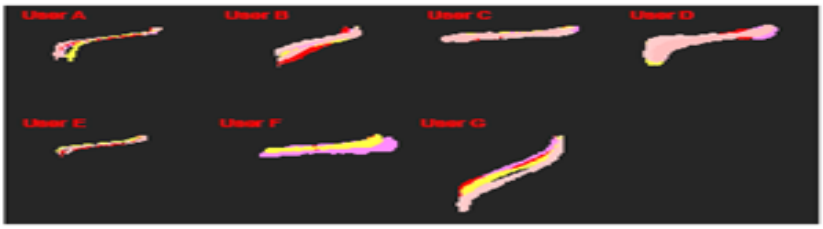
FAST collects elected touch gesture information including gesture their type, X and Y coordinates, directions of the finger motion, speed of finger motion, pressure at each sampled touch point and the distance between multi-touch points .We select only the six most frequent and useful gestures: DU (Down to Up) swipe, UP (Up to Down) swipe, LR (Left to right) swipe, RL (right to left) swipe, zoom in, and zoom-out. Since a Smartphone user may apply different levels of touch pressure at different stages of a touch gesture FAST also divides each gesture into three parts, (i) Start of a touch motion, (ii) the main touch motion, which are the longest segment and (iii) the end of a touch motion.[9].



(a) Sample Spread Profiles of Seven Users



(b) Sample Pinch Profiles of Seven Users



(c) Sample Flick Profiles of Seven Users

Fig.3 –Sample Gesture patterns [7]

In above samples of gestures in figure3- (a), figure (b), figure(c) number of patterns is considered. For each trace pressure is calculated by considering the number of dots glow at the time of gesture is draw. This process of calculation of pressure is simple and it calculated depends on the glow of dots. The glove provides X, Y, and Z axis pointed rate information, pitch and roll of finger movements, for a total of 36 additional features. It uses these features to validate and complement touch gesture extracted features, for the user authentication process that occurs during normal Smartphone interactions.

3.2 FAST (Finger gesture Authentication system using Touchscreen)

FAST extracts steady touch pressure, minor/major ratio, steady finger moving speed, and acceleration/de-acceleration speed as features. FAST uses a digital sensor glow to collect this information. FAST collects, separates and stores the above three types of data, into two databases. One database is used for training classifiers and the other for testing the trained classifiers. Collected touch inputs are split FAST uses classifiers to classify different mobile touch screen devices data it uses three classifications Algorithms, (i) Decision tree (ii) Random Forest and (iii) Bayes net classifier[9].

FAST store, separate and collect the all three type data which are required for the user authentication in the mobile into two databases. The database uses the three classifier algorithms for sorting the data collected from the user. FAST uses the results of the classifiers for the improving the security of the mobile. FAST provide the security to mobile by using the post-login stage, FAST extracts touch gesture and digital sensor glove features and uses them to authenticate the mobile user. FAST take more care about to maintain a proper balance of the FAR (False Acceptance Rate) and FRR (False Rejection Rate) values. Due to the continuous monitoring and sequential authentication process the FRR is maintained for improving the efficiency of the mobile security.

FAST uses two metrics: (i) the Touch Sequence Length (TSL), the length of touch input sequences (ii) The Authentication Threshold (AT), for aggregating results. The AT metric is used to provide the lower bound on the touch sequence length: If the number of accepted touch inputs during one sequence is below the threshold, FAST considers that the current user is unauthorized and invokes an explicit authentication process. FAST continuously monitors the authenticity of the mobile user in a user transparent fashion. FAST achieves this by intercepting touch gestures and virtual typing inputs, and strives to achieve a low FRR. The post-login stage, due to the constant user monitoring and frequent transparent authentication based on touch gestures and sensor glove inputs.

IV. SEQUENCE BASD GESTURE AUTHENTICATION

In sequence based gesture authentication firstly user provides a more than one gestures to the touchscreen Smartphone devices and a sequence or order is given to the each gesture this data is stored in the database. There is time threshold is given between each gesture is sixty seconds and it also considers the pressure of the trace at the time of gesture draw. The pressure is calculated by using sensor glow which calculated on the number of dots or pixels are glow at the time of trace draw. When user use their Smartphone device at that time user require to give more than one gesture and their order within the time threshold if all these three thing are match with the registered things then user will be authenticate

otherwise user will be considered as unauthorized user and his access will be denied. This process helps to provide the strong security because more than one gesture provide to the mobile authentication.

V. CONCLUSION

This paper is the review of the continuous mobile authentication using a multiple gesture in touchscreen handheld devices with the FAST (Finger gestures Authentication System using Touchscreen) authentication technique, this proposed system provides the strong security to the touch based handheld devices by using sequence of multiple gesture and time limitation.

REFERENCES

[1] Worldwide smartphone markets: 2011 to 2015 - analysis, data, insight and forecasts. http://www.researchandmarkets.com/research/7a1189/worldwide smartphone.

[2] More top worst passwords. http://xato.net/passwords/ more-top-worst-passwords#more-269, 2010

[3] http://finance.yahoo.com/news/biometric-authentication-provides-better-mobile-155900395.html

[4] Security Precautions for Mobile Handheld Devices http://www.it.cornell.edu/security/computer/mobile.cfm#conf

[5] Master Thesis: *"Gesture-based User Authentication on Mobile Devices using Accelerometer and Gyroscope" 8th August 2011*

[6] A. J. Aviv, K. Gibson, E. Mossop, M. Blaze, and J. M.Smith, "Smudge attacks on smartphone touch screens" In Proceedings of the 4th USENIX conference on Offensive technologies, WOOT'10, CA, USA, 2010. USENIX Association

[7] M. Frank, R. Biedert, E. Ma, I. Martinovic, and D. Song. Touchalytics: "*On the applicability of touchscreen input as a Behavioural biometric for continuous authentication".*Information Forensics and Security, *IEEE Transactions on, 8(1):136–148, 2013.*

[8] Tao Feng, Ziyi Liu Kyeong-An Kwon, Weidong Shi, Bogdan Carbunary, Yifei Jiangz and Nhung Nguyen Computer Science Department, University of Houston "*Continuous Mobile Authentication using Touchscreen Gestures",* 2012

[9] N. Kirschnick, S. Kratz, and S. Moller. *An improved approach to gesture-based authentication for mobile devices*. In Proc. Symp. Usable Privacy and Security, SOUPS '10, 2010.

[10] N. Sae-Bae, K. Ahmed, K. Isbister, and N. Memon. Biometric-rich gestures: "*A novel approach to authentication on*

[11] *Multi-touch devices*. In Proc. ACM Conf. Human Factors in Computing Systems (CHI'12), pages 977-986, 2012.

